PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-011101

(43)Date of publication of application : 14.01.2000

(51)Int.Cl. G06K 17/00
G06F 3/06
G06F 3/08
G06K 19/073
G06K 19/07

(21)Application number : 10-173163

(22)Date of filing : 19.06.1998

(71)Applicant : HITACHI LTD

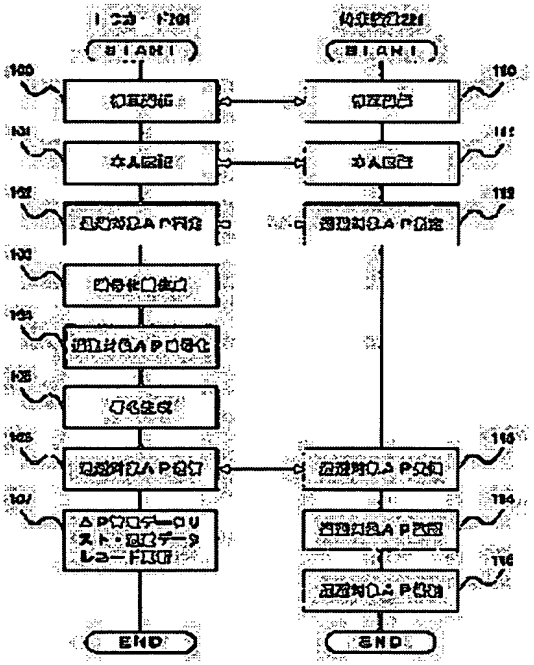
(72)Inventor : FUKUZAWA YASUKO
ORIMO MASAYUKI
HARAGUCHI MASATOSHI

(54) IC CARD AND RECORD MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To save an application program(AP) stored in an IC card according to the judgment of a user, and to prevent the illegal use of the saved AP.

SOLUTION: An IC card 201 generates and manages an arbitrary cryptographic key, and enciphers an AP to be saved among APS stored in an internal memory by using this cryptographic key, and saves this AP through an IC card reader/writer 211 to a connected terminal equipment 221, and deletes the AP before encipherment. Also, at the time of restoring the saved AP, the IC card 201 decodes the AP received from the terminal equipment 221 by using the managed cryptographic key, and restores the AP in the internal memory.



LEGAL STATUS

[Date of request for examination] 15.08.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or

application converted registration]	
[Date of final disposal for application]	
[Patent number]	3597704
[Date of registration]	17.09.2004
[Number of appeal against examiner's decision of rejection]	
[Date of requesting appeal against examiner's decision of rejection]	
[Date of extinction of right]	

[JP2000-011101]

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the technique which carries out operational administration of the IC card with which one or more data is stored, and relates to the technique of showing the solution over security needs especially.

[0002]

[Description of the Prior Art] Conventionally only the data which an application program ("AP" is called hereafter.) uses were stored in the IC card, and the utilization gestalt it was made to operate AP was common at the terminal unit side which read this data through IC card reader / writer.

[0003] On the other hand, the motion which stores AP in an IC card is becoming large by storing the operating system (card OS) for operating AP on an IC card in recent years in an IC card.

[0004] Moreover, two or more AP is stored in the IC card of one sheet, operability is raised by unifying two or more IC cards to the IC card of one sheet, and carrying out the share of the cost of an IC card in AP issuance engine is expected.

[0005] In addition, MULTOS is known as an example of Card OS.

[0006] Each AP divided, and was recorded by the special fire wall program, and MULTOS has guaranteed that other AP does not block actuation while various AP outputted to the IC card confirms whether to be what loading to an IC card was permitted correctly as description is made by reference called Fuji-Keizai USA "the trend of the electronic advance card in Japan, the U.S. and Europe, and a future direction." In order that loading to an IC card may confirm whether to be what was permitted correctly, in advance of loading of AP, a management engine verifies the justification of AP and performs processing which guarantees being loaded only to a normal user's IC card. Since deletion of AP loaded to the IC card as well as loading is performed after checking it, it needs to guarantee the justification of deletion from the IC card which this ** with a management engine.

[0007]

[Problem(s) to be Solved by the Invention] MULTOS cannot load AP without a management engine's permission to an IC card, but since it can prevent copying AP to an IC card indefinitely and it can realize effective management, it is spreading as a card OS.

[0008] However, according to the utilization situation of an IC card, such strict management is decision

of a user and will restrict flexible employment to which only specific AP is evacuated temporarily from the IC card with which two or more AP was stored.

[0009] For example, to recover AP to which evacuated AP which is not needed for a while from the IC card, evacuated AP stored in the IC card by decision of a user, and cancelled from the time of a third party using an IC card temporarily, constraint of the amount of memory, etc. to replace with other AP to use, and it was made to evacuate is desired.

[0010] However, since a management engine's permission is needed also at the time of deletion of AP from an IC card as MULTOS was mentioned above in the IC card used as Card OS, employment to which it is decision of a user and AP is evacuated temporarily cannot be performed.

[0011] The object of this invention is to make it possible to prevent the unauthorized use of the data to which it is made to have evacuated while making it possible to evacuate the data stored in the IC card by decision of a user.

[0012]

[Means for Solving the Problem] In order to attain the above-mentioned object, this invention enciphers the data stored in the IC card within an IC card using the encryption key generated within the IC card, and he is trying to evacuate the data after encryption from an IC card. Moreover, the generated encryption key is managed within the IC card, and in case the data to which it was made to evacuate are recovered, he is trying to decode this data within an IC card using the encryption key managed within the IC card.

[0013] Namely, a means to receive from the outside the assignment of data which this invention is an IC card with which one or more data is stored in internal memory as the 1st mode, and is made applicable to evacuation, While enciphering using the generated encryption key, a means to generate the encryption key of arbitration, and the data received as an object for evacuation A means to eliminate the data before encryption, and a means to memorize the generated encryption key, A means to evacuate the data after encryption outside, and a means to receive the data to which it was made to evacuate from the exterior, The IC card characterized by having a means to decode the received data using the memorized encryption key, and a means to re-store the data after decode in internal memory is offered.

[0014] According to the 1st mode, since it cannot decode except the IC card which enciphered this, being used improperly of the data to which it was evacuated from the IC card is lost.

[0015] What is necessary is just to make it transpose to the data after enciphering the data before encryption here, when the enciphered data do not need to be evacuated from an IC card.

[0016] Namely, a means to receive from the outside the assignment of data which this invention is an IC card with which one or more data is stored in internal memory as the 2nd mode, and is made applicable to nullification, While enciphering using the generated encryption key, a means to generate the encryption key of arbitration, and the data received as an object for nullification The means replaced with the data after enciphering the data before encryption, and a means to memorize the generated encryption key, The IC card characterized by having a means to receive from the outside the assignment of data made applicable to validation, and a means to decode the data received as an object for validation using the memorized encryption key is offered.

[0017] in addition, the 1st mode and the 2nd voice -- an IC card [like] -- naturally also in any, it comes

out of one or more data stored in internal memory that AP can be included.

[0018]

[Embodiment of the Invention] Hereafter, the gestalt of operation of this invention is explained with reference to a drawing.

[0019] Drawing 2 is the whole IC card system block diagram concerning this operation gestalt.

[0020] As shown in drawing 2 , IC card system concerning this operation gestalt has the composition that IC card 201 which a user owns, and the terminal unit 221 were connected through IC card reader / writer 211.

[0021] IC card 201 is equipped with MPU203, memory 202, and transmission and reception IF 204, and is constituted, and a terminal unit 221 is equipped with MPU223, memory 222, a keyboard 224, a display 225, and transmission and reception IF 226, and is constituted.

[0022] Moreover, IC card reader / writer 211 is equipped with transmission and reception IF 212 and transmission and reception IF 213, and is constituted.

[0023] Although IC card 201 and a terminal unit 221 transmit and receive through IC card reader / writer 211, a communicative gestalt does not ask a cable/wireless.

[0024] Next, the content stored in the memory 202 of IC card 201 is explained using drawing 3 .

[0025] Although or more 1AP, such as a credit and GSM (global system for mobile communication), is stored in the memory 202 of IC card 201 as shown in drawing 3 , AP#1 (321) and AP#2 (322) shall be stored here.

[0026] Moreover, as shown in drawing 3 , the card identity child 311 who is an identifier of a proper, the public key 312 of the certificate authority in an unsymmetrical code, the private key 313 of IC card 201 in an unsymmetrical code, the public key 314 of IC card 201 in an unsymmetrical code, the AP management information 315, and the password 316 for permitting access to IC card 201 are stored in the memory 202 of IC card 201 every IC card 201.

[0027] Drawing 7 is drawing showing an example of the AP management information 315.

[0028] The AP management information 315 consists of AP managed data lists 700 corresponding to each of AP (here, it is AP#1 (321) and AP#2 (322).) stored in the memory 202 of IC card 201.

[0029] As shown in drawing 7 , the AP managed data list 700 of AP#1 (321) The AP identifier 701 which is an identifier of AP#1 (321), and the AP file information 702, The load counter 703 which shows the count which loaded AP#1 (321) to IC card 201, The deletion counter 704 which shows the count which deleted [201] AP#1 (321), It consists of a pointer 705 to the evacuation data record 800 shown in drawing 8 , and an entry pointer 706 to the AP managed data list 700 of AP#2 (322) which is following AP.

[0030] In addition, the AP managed data list 700 of AP#2 (322) is also the same configuration.

[0031] Moreover, "NULL" is set up, and if it becomes, if corresponding AP to which corresponding AP is not evacuated is evacuated, the pointer to the evacuation data record 800 will be set to a pointer 705, when evacuation of AP is completed. In addition, about the detail of the evacuation data record 800, it mentions later.

[0032] It returns to drawing 3 and AP evacuation program 303, AP recovery program 304, the encryption key generator 305, the signature generator 306, symmetry cryptosystem encryption / decode program 307, and unsymmetrical cryptosystem encryption / decode program 308 are stored in

the memory 202 of IC card 201.

[0033] Next, the content stored in the memory 222 of a terminal unit 221 is explained using drawing 4 .

[0034] As shown in drawing 4 , the terminal identification child 411 who is an identifier of a proper, and the public key 412 of the certificate authority in an unsymmetrical code are stored in the memory 222 of a terminal unit 221 every terminal unit 221.

[0035] Moreover, as shown in drawing 4 , AP evacuation program 403, AP recovery program 404, the signature verification program 405, symmetry cryptosystem encryption / decode program 406, and unsymmetrical cryptosystem encryption / decode program 407 are stored in the memory 222 of a terminal unit 221.

[0036] In addition, although it is possible that the various data stored in the memory 202 of IC card 201 and the memory 222 of a terminal unit 211 form generation / issuance / management engine respectively, the various data containing the public key (public key with which the signature was performed by the certificate authority) attested by the certificate authority which generally exists shall already be set up here.

[0037] Next, in IC card system concerning this operation gestalt, the actuation at the time of evacuating AP stored in IC card 201 to a terminal unit 221 is explained using drawing 1 .

[0038] Drawing 1 is drawing showing the flow of the actuation at the time of AP evacuation in IC card system concerning this operation gestalt.

[0039] If AP evacuation program 403 is started with a terminal unit 221 and IC card 201 is inserted in IC card reader / writer 211, AP evacuation program 303 will be started with IC card 201, and the following processings will be performed. In addition, the following processings are realized because MPU203 of IC card 201 and MPU223 of a terminal unit 221 perform AP evacuation program 303 and AP evacuation program 403.

[0040] First, IC card 201 and a terminal unit 211 perform mutual recognition (step 100, step 110). Since the authentication method which the authentication method which used the unsymmetrical key code is specified to ISO (ISO 9798-3) about mutual recognition, for example, and used the symmetry key code for ISO (ISO 9798-2) is specified, a detail is omitted here.

[0041] then, IC card 201 and a terminal unit 211 -- a principal -- it attests (step 101, step 111).

[0042] In principal authentication, in detail, first, a terminal unit 221 requires the input of a password of a user through a display 225, and the password which the user entered from the keyboard 224 is transmitted to IC card 201 (step 111).

[0043] And if IC card 201 receives a password from a terminal unit 211, it will compare the received password with the password 316 stored in memory 202, and will attest whether you are a right user (step 101). In addition, the authentication result by IC card 201 is notified to a terminal unit 211.

[0044] Now, when it is attested that he is a right user, IC card 201 and a terminal unit 211 specify the object AP for evacuation (step 102, step 112).

[0045] In assignment for [AP] evacuation, in detail, a terminal unit 221 acquires the list of AP stored in IC card 201 from IC card 201, and displays it on a display 225 first, and AP which the user specified from the keyboard 224 is notified to IC card 201 as an object AP for evacuation (step 112). In addition, advice for [AP] evacuation is performed by transmitting AP assignment data record 500 shown in drawing 5 .

[0046] Drawing 5 is drawing showing an example of AP assignment data record 500.
[0047] As shown in drawing 5 , AP assignment data record 500 consists of an AP identifier 501 which is an identifier for specifying the object AP for evacuation as a meaning, a terminal identification child (terminal identification child 411 stored in memory 222) 502 of a terminal unit 221, and a time stump 503 in which the time in which the terminal unit 221 received assignment for [AP] evacuation is shown.
[0048] And IC card 201 receives assignment for [AP] evacuation by receiving AP assignment data record 500 from a terminal unit 211 (step 102).
[0049] Then, IC card 201 will generate the encryption key for enciphering the object AP for evacuation by starting the encryption key generator 305, if AP assignment data record 500 is received (step 103). Here, the encryption key which enciphers and generates the object AP for evacuation in a symmetry code is an encryption key (for example, random number) in a symmetry code.
[0050] Then, IC card 201 eliminates AP before encryption while enciphering the object AP for evacuation using the encryption key generated at step 103 by starting symmetry cryptosystem encryption / decode program 308 (step 104).
[0051] Then, IC card 201 generates a signature by starting the signature generator 306 (step 105).
[0052] At step 105, in detail, by generating an authentication child using a Hash Function and starting unsymmetrical cryptosystem encryption / decode program 308 from the data record 900 for signature generation shown in drawing 9 , IC card 201 enciphers the authentication child who generated using the private key 313 of IC card 200 stored in memory 202, and generates a signature. In addition, refer to work "a present age code" besides for example, Tatsuaki Okamoto, and the Sankei books issuance for the detail of a Hash Function and signature generation.
[0053] Drawing 9 is drawing showing an example of the data record 900 for signature generation.
[0054] As shown in drawing 9 , the data record 900 for signature generation The object AP 902 for evacuation enciphered as the AP identifier 901 for [AP] evacuation With the terminal identification child 903 (terminal identification child 502 in AP assignment data record 500 received from the terminal unit 221) It consists of a time stump (time stump 503 in AP assignment data record 500 received from the terminal unit 221) 904, and a card identity child (card identity child 313 stored in memory 202) 905 of IC card 201.
[0055] Then, IC card 201 and a terminal unit 211 transmit and receive the enciphered object AP for evacuation (step 106, step 113).
[0056] In transmission and reception for [which was enciphered / AP] evacuation, the object AP for evacuation which IC card 201 enciphered is first transmitted to a terminal unit 221 in detail (step 106). In addition, transmission for [which was enciphered / AP] evacuation is performed by transmitting the evacuation AP data record 600 shown in drawing 6 R> 6.
[0057] Drawing 6 is drawing showing an example of the evacuation AP data record 600.
[0058] As shown in drawing 6 , the evacuation AP data record 600 consists of the AP identifier 601 for [which was enciphered / AP] evacuation, the card identity child (card identity child 313 stored in memory 202) 603 of IC card 201 for [AP / 602] evacuation who enciphered at step 104, signature 604 generated at step 105, and a public key 605 (public key 314 stored in memory 202) of IC card 201.

[0059] And a terminal unit 221 receives the enciphered object AP for evacuation by receiving the evacuation AP data record 600 from IC card 201 (step 113).
[0060] Now, a terminal unit 221 will verify the signature 604 in the evacuation AP data record 600 by starting the signature verification program 405, if the evacuation AP data record 600 is received (step 114).
[0061] At step 114, in detail, by starting unsymmetrical cryptosystem encryption / decode program 407, first, a terminal unit 221 decodes the public key 605 in the evacuation AP data record 600 using the public key 412 of a certificate authority, verifies a public key 605, then decodes the signature 604 in the evacuation AP data record 600 using the verified public key 605, and verifies signature 604.
[0062] And a terminal unit 221 stores the evacuation AP data record 600 in memory 222 or a disk unit, if it checks that the evacuation AP data record 600 is transmitted from IC card 201, and that the evacuation AP data record 600 is not altered as a result of verification by step 114 (step 115). In addition, a terminal unit 221 notifies the purport that it succeeded in evacuation of AP to IC card 201.
[0063] Then, IC card 201 will update the corresponding AP managed data list 700, if the purport that it succeeded in evacuation of AP is notified from a terminal unit 221 (step 107).
[0064] At step 107, IC card 201 generates the evacuation data record 800, and, specifically, sets the pointer to the generated evacuation data record 800 as the pointer 705 in the corresponding AP managed data list 700.
[0065] Drawing 8 is drawing showing an example of the evacuation data record 800.
[0066] As shown in drawing 8 , the evacuation data record 800 consists of the terminal identification child (terminal identification child 502 in AP assignment data record 500 received from the terminal unit 221) 801, a time stump (time stump 503 in AP assignment data record 500 received from the terminal unit 221) 802, an encryption key 803 generated at step 103, and signature 804 generated at step 105.
[0067] By actuation explained above, AP stored in IC card 201 can be evacuated to a terminal unit 221.
[0068] In addition, although he is trying to encipher the object AP for evacuation in a symmetry code, you may make it encipher the object AP for evacuation in an unsymmetrical code in the actuation shown in drawing 1 . In this case, IC card 201 generates the encryption key according to the algorithm of an unsymmetrical code at step 103.
[0069] Moreover, since they can share a key temporarily, they may temporarily [this] be made for IC card 201 and a terminal unit 221 to be the processes of the mutual recognition of step 100 and step 110, and to carry out cryptocommunication of the evacuation AP data record 600 in the actuation shown in drawing 1 , using a key.
[0070] Moreover, you may make it a terminal unit 221 store the evacuation AP data record 600 in the location which it is made to make a user specify an evacuation location, and the user specified from the keyboard 224 in the actuation shown in drawing 1 .
[0071] Moreover, in the actuation shown in drawing 1 , although he is trying to check that the evacuation AP data record 600 is transmitted from IC card 201, and that the evacuation AP data record 600 is not altered using the authentication technique by signature in order to raise security nature more, the main point of this invention is not limited by this.

[0072] Next, in IC card system concerning this operation gestalt, the actuation at the time of recovering AP to which it was made to evacuate in the actuation shown in drawing 1 is explained using drawing 10 .

[0073] Drawing 10 is drawing showing the flow of the actuation at the time of AP recovery in IC card system concerning this operation gestalt.

[0074] If AP recovery program 404 is started with a terminal unit 221 and IC card 201 is inserted in IC card reader / writer 211, AP recovery program 304 will be started with IC card 201, and the following processings will be performed. In addition, the following processings are realized because MPU203 of IC card 201 and MPU223 of a terminal unit 221 perform AP recovery program 304 and AP recovery program.

[0075] first, the actuation which explained IC card 201 and the terminal unit 211 by drawing 1 -- the same -- mutual recognition -- carrying out (step 100, step 110) -- a principal -- it attests (step 101, step 111).

[0076] And when it is attested that he is a right user, IC card 201 and a terminal unit 211 specify the object AP for recovery (step 1002, step 1012).

[0077] In assignment for [AP] recovery, in detail, a terminal unit 221 acquires the list of AP under evacuation of AP stored in IC card 201 from IC card 201, and displays it on a display 225 first, and AP which the user specified from the keyboard 224 is notified to IC card 201 as an object AP for recovery (step 1012). In addition, advice for [AP] recovery is performed by transmitting AP assignment data record 500 like advice for [AP] evacuation.

[0078] And IC card 201 receives assignment for [AP] recovery by receiving AP assignment data record 500 from a terminal unit 211 (step 1002).

[0079] Then, IC card 201 will take out the evacuation data record 800 which the pointer 705 in the AP managed data list 700 for [AP] recovery and this AP managed data list 700 shows, if AP assignment data record 500 is received (step 1003).

[0080] Then, IC card 201 and a terminal unit 211 transmit and receive the object AP for recovery (step 1004, step 1013).

[0081] In transmission and reception for [AP] recovery, a terminal unit 211 transmits in detail the evacuation AP data record 600 stored in memory 222 or a disk unit to a terminal unit 221 as an object AP for recovery first (step 1013). And IC card 201 receives the object AP for recovery by receiving evacuation AP data from a terminal unit 211 (step 1004).

[0082] Now, it checks whether if the evacuation AP data record 600 is received, the signature 604 in the evacuation AP data record 600 and the signature 804 of IC card 201 in the evacuation data record 800 taken out at step 1003 correspond (step 1005).

[0083] If it checks that both of IC card 201 correspond, and by starting symmetry cryptosystem encryption / decode program 307 The encryption AP 602 in the received evacuation AP data record 600 is decoded using the encryption key 803 in the evacuation data record 800 taken out at step 1003. The decoded object AP for recovery is rearranged in memory 202 according to the file information 702 in the AP managed data list 700 taken out at step 1003 (step 1006).

[0084] Furthermore, IC card 201 updates the AP managed data list 700 for [AP] recovery (step 1007).

[0085] At step 1007, IC card 201 eliminates the evacuation data record 800 taken out at step 1003, and, specifically, sets "NULL" as the pointer 705 in the AP managed data list 700 for [AP] recovery.
[0086] IC card 201 can be made to recover AP which made it evacuate to a terminal unit 221 by actuation explained above.
[0087] As explained above, according to the IC card system concerning this operation gestalt, it becomes possible to evacuate AP stored in IC card 201 to a terminal unit 221 from IC card 201 by decision of a user. And since he is trying to encipher using the encryption key which generated the object AP for evacuation within IC card 201, except IC card 201 which enciphered this, AP evacuated from IC card 201 cannot be decoded, and is not used improperly.
[0088] Then, even when IC card 201 is using MULTOS as Card OS especially, performing actuation shown in drawing 1 can realize flexible employment to which AP is evacuated temporarily by decision of a user.
[0089] By the way, in IC card system concerning this operation gestalt, although he is trying to evacuate AP stored in IC card 201 to a terminal unit 221, AP can be temporarily cancelled within IC card 201 instead of evacuating AP, when AP enciphered when allowances were in the memory 202 of IC card 201 does not need to be evacuated from IC card 201.
[0090] Hereafter, the actuation at the time of doing in this way is explained using drawing 11 .
[0091] Drawing 11 is drawing showing the flow of the actuation at the time of AP nullification in IC card system concerning this operation gestalt.
[0092] Although the actuation shown in drawing 11 is the same as the actuation shown in drawing 1 , in step 1106, it differs in that AP which IC card 201 enciphered was stored in IC card 201. Then, in the various data mentioned above, nothing will be set to the part which was required evacuation / in order to make it recover.
[0093] According to the actuation shown in drawing 11 , although AP is not evacuated actually, since AP is enciphered within IC card 201, it can protect from a third party's threat.
[0094] In addition, IC card 201 should just decode the actuation at the time of validating cancelled AP using the encryption key which used AP enciphered and cancelled when this was enciphered.
[0095] Moreover, to be made to perform actuation shown in drawing 11 , it is necessary to make it make a user specify selection of whether AP is evacuated or it is made to cancel in a terminal unit 221.
[0096] Moreover, actuation shown in drawing 11 can be carried out independently of the actuation shown in drawing 1 . That is, it is possible to build IC card system which performs only actuation shown in drawing 1111 .
[0097] In addition, by the above explanation, although the data made applicable [for evacuation] to nullification shall be AP, it is not necessary to explain that you may be other data other than AP.
[0098]
[Effect of the Invention] As explained above, according to this invention, it becomes possible to evacuate the data stored in the IC card from an IC card by decision of a user. And except the IC card which enciphered this, the data to which AP to which it is made to evacuate was evacuated from the IC card since he was trying to encipher using the encryption key generated within the IC card cannot be decoded, and are not used improperly.

CLAIMS

[Claim(s)]

[Claim 1] A means to receive from the outside the assignment of data which one or more data is the IC cards stored in internal memory, and is made applicable to evacuation, While enciphering using the generated encryption key, a means to generate the encryption key of arbitration, and the data received as an object for evacuation A means to eliminate the data before encryption, and a means to memorize the generated encryption key, The IC card characterized by having a means to evacuate the data after encryption outside, a means to receive the data to which it was made to evacuate from the exterior, a means to decode the received data using the memorized encryption key, and a means to re-store the data after decode in internal memory.

[Claim 2] A means to receive from the outside the assignment of data which one or more data is the IC cards stored in internal memory, and is made applicable to nullification, While enciphering using the generated encryption key, a means to generate the encryption key of arbitration, and the data received as an object for nullification The means replaced with the data after enciphering the data before encryption, and a means to memorize the generated encryption key, The IC card characterized by having a means to receive from the outside the assignment of data made applicable to validation, and a means to decode the data received as an object for validation using the memorized encryption key.

[Claim 3] One or more data which are IC cards according to claim 1 or 2, and are stored in internal memory is IC cards characterized by including an application program.

[Claim 4] It is the record medium which recorded the program installed in the terminal unit to which an IC card according to claim 1 is connected through IC card reader / writer. While receiving assignment of the data set as the evacuation object of the one or more data stored in the above-mentioned IC card A means to output the received content of assignment to the above-mentioned IC card, and a means to receive the data to which it was evacuated from the above-mentioned IC card, and to store in the memory of the above-mentioned terminal unit, A means to receive assignment of the data set as the recovery object of the data which are evacuated from the above-mentioned IC card and stored in the above-mentioned terminal unit, The record medium characterized by recording the program operated so that the above-mentioned terminal unit may be equipped with a means to output the data received as an object for recovery to the above-mentioned IC card.

[Claim 5] It is the record medium which recorded the program installed in the terminal unit to which an IC card according to claim 2 is connected through IC card reader / writer. While receiving assignment of the data set as the nullification object of the one or more data stored in the above-mentioned IC card While receiving assignment of the data set as the validation object of a means to output the received content of assignment to the above-mentioned IC card, and the data stored in the above-mentioned IC card The record medium characterized by recording the program operated so that the above-mentioned terminal unit may be equipped with a means to output the received content of assignment to the above-mentioned IC card.

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2000－11101
（P2000－11101A）
(43)公開日　平成12年１月14日(2000.1.14)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｂ	５Ｂ０３５
			Ｅ	５Ｂ０５８
Ｇ０６Ｆ　3/06	３０４	Ｇ０６Ｆ　3/06	３０４Ｈ	５Ｂ０６５
3/08		3/08	Ｃ	
Ｇ０６Ｋ　19/073		Ｇ０６Ｋ　19/00	Ｐ	

審査請求　未請求　請求項の数５　ＯＬ　（全 10 頁）　最終頁に続く

(21)出願番号　特願平10－173163

(22)出願日　平成10年６月19日(1998.6.19)

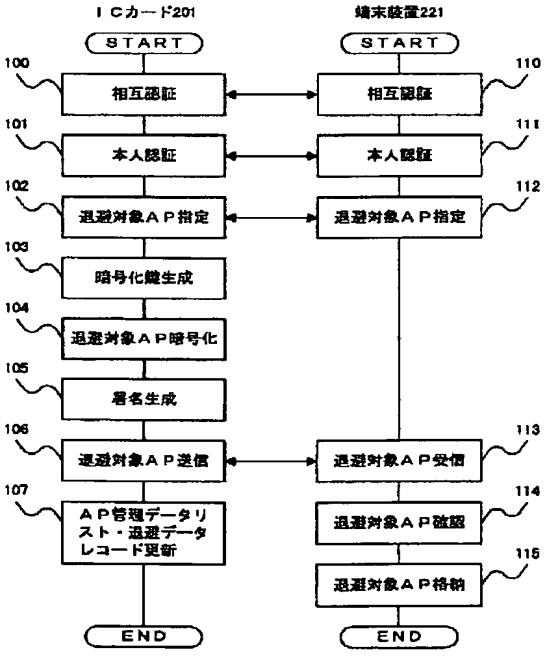
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　福澤　寧子
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　織茂　昌之
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(74)代理人　100087170
弁理士　富田　和子

最終頁に続く

(54)【発明の名称】　ＩＣカードおよび記録媒体

(57)【要約】
【課題】ＩＣカードに格納されているアプリケーションプログラム（ＡＰ）を、ユーザの判断で退避させることを可能とすると共に、退避させてあるＡＰの不正使用を防止する。
【解決手段】ＩＣカード２０１は、任意の暗号化鍵を生成して管理し、内部のメモリ２０２に格納されているＡＰのうちの、退避対象とするＡＰを、この暗号化鍵を用いて暗号化してから、ＩＣカードリーダ／ライタ２１１を介して接続される端末装置２２１に退避させ、暗号化前のＡＰを消去する。また、ＩＣカード２０１は、退避させておいたＡＰを回復させる際には、端末装置２２１から受け取ったＡＰを、管理しておいた暗号化鍵を用いて復号し、内部のメモリ２０２に再格納する。

図　1



【特許請求の範囲】
【請求項１】１つ以上のデータが内部のメモリに格納されているＩＣカードであって、
退避対象とするデータの指定を外部から受け付ける手段と、
任意の暗号化鍵を生成する手段と、
退避対象として受け付けたデータを、生成した暗号化鍵を用いて暗号化すると共に、暗号化前のデータを消去する手段と、
生成した暗号化鍵を記憶する手段と、
暗号化後のデータを外部に退避させる手段と、
退避させておいたデータを外部から受け取る手段と、
受け取ったデータを、記憶しておいた暗号化鍵を用いて復号する手段と、
復号後のデータを内部のメモリに再格納する手段とを備えたことを特徴とするＩＣカード。
【請求項２】１つ以上のデータが内部のメモリに格納されているＩＣカードであって、
無効化対象とするデータの指定を外部から受け付ける手段と、
任意の暗号化鍵を生成する手段と、
無効化対象として受け付けたデータを、生成した暗号化鍵を用いて暗号化すると共に、暗号化前のデータを暗号化後のデータに置き換える手段と、
生成した暗号化鍵を記憶する手段と、
有効化対象とするデータの指定を外部から受け付ける手段と、
有効化対象として受け付けたデータを、記憶しておいた暗号化鍵を用いて復号する手段とを備えたことを特徴とするＩＣカード。
【請求項３】請求項１または２記載のＩＣカードであって、
内部のメモリに格納されている１つ以上のデータは、アプリケーションプログラムを含むことを特徴とするＩＣカード。
【請求項４】請求項１記載のＩＣカードがＩＣカードリーダ／ライタを介して接続される端末装置にインストールされるプログラムを記録した記録媒体であって、
上記ＩＣカードに格納されている１つ以上のデータのうちの、退避対象となるデータの指定を受け付けると共に、受け付けた指定内容を上記ＩＣカードに出力する手段と、
上記ＩＣカードから退避させられたデータを受け取って、上記端末装置のメモリに格納する手段と、
上記ＩＣカードから退避させられて上記端末装置に格納されているデータのうちの、回復対象となるデータの指定を受け付ける手段と、
回復対象として受け付けたデータを上記ＩＣカードに出力する手段とを、上記端末装置が備えるよう動作させるプログラムを記録したことを特徴とする記録媒体。
【請求項５】請求項２記載のＩＣカードがＩＣカードリーダ／ライタを介して接続される端末装置にインストールされるプログラムを記録した記録媒体であって、
上記ＩＣカードに格納されている１つ以上のデータのうちの、無効化対象となるデータの指定を受け付けると共に、受け付けた指定内容を上記ＩＣカードに出力する手段と、
上記ＩＣカードに格納されているデータのうちの、有効化対象となるデータの指定を受け付けると共に、受け付けた指定内容を上記ＩＣカードに出力する手段とを、上記端末装置が備えるよう動作させるプログラムを記録したことを特徴とする記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、１つ以上のデータが格納されているＩＣカードを運用管理する技術に係り、特に、セキュリティニーズに対する解決策を提示する技術に関するものである。
【０００２】
【従来の技術】従来は、アプリケーションプログラム（以下、「ＡＰ」と称す。）が利用するデータのみをＩＣカードに格納しておき、ＩＣカードリーダ／ライタを介してこのデータを読み取った端末装置側で、ＡＰを動作させるようにした利用形態が一般的であった。
【０００３】これに対し、近年、ＩＣカード上でＡＰを動作させるための基本ソフト（カードＯＳ）をＩＣカードに格納することで、ＡＰをＩＣカードに格納する動きが大きくなりつつある。
【０００４】また、複数のＡＰを１枚のＩＣカードに格納し、複数のＩＣカードを１枚のＩＣカードに統合することで、操作性を向上させ、ＩＣカードのコストを、ＡＰ発行機関でシェアすることが期待されている。
【０００５】なお、カードＯＳの一例としては、ＭＵＬＴＯＳが知られている。
【０００６】ＭＵＬＴＯＳは、Fuji - Keizai ＵＳＡ「日米欧における電子アドバンス・カードのトレンドと今後のディレクション」という文献に記述がなされているように、ＩＣカードに出力された様々なＡＰが、ＩＣカードへのロードを正しく許可されたものか否かをチェックすると共に、個々のＡＰが、特殊なファイアウォール・プログラムによって分割して記録され、他のＡＰが動作を妨害しないことを保証している。ＩＣカードへのロードが正しく許可されたものか否かをチェックするために、ＡＰのロードに先立って、管理機関は、ＡＰの正当性を検証し、正規利用者のＩＣカードにのみロードされることを保証する処理を行う。ＩＣカードにロードされたＡＰのデリートも、ロードと同様にチェックしてから行われるため、管理機関によって、該等するＩＣカードからのデリートの正当性を保証する必要がある。
【０００７】

【発明が解決しようとする課題】ＭＵＬＴＯＳは、管理機関の許可のないＡＰをＩＣカードにロードすることができず、ＡＰがＩＣカードに無制限にコピーされることを防ぐことができるので、有効な管理を実現することができることから、カードＯＳとして普及していきつつある。

【０００８】しかしながら、このような厳密な管理は、ＩＣカードの利用状況に応じて、ユーザの判断で、複数のＡＰが格納されたＩＣカードから、特定のＡＰだけを一時的に退避させるような、フレキシブルな運用を制限してしまう。

【０００９】例えば、第三者が一時的にＩＣカードを利用するときや、メモリ量の制約などから、しばらく必要としないＡＰをＩＣカードから退避させ、使用したい他のＡＰと置き換えたい場合には、ユーザの判断で、ＩＣカードに格納されているＡＰを退避させて無効化し、また、退避させておいたＡＰを回復させることが望まれる。

【００１０】しかし、ＭＵＬＴＯＳをカードＯＳとしているＩＣカードにおいては、上述したように、ＩＣカードからのＡＰのデリート時にも管理機関の許可を必要とするので、ユーザの判断で、一時的にＡＰを退避させるような運用はできない。

【００１１】本発明の目的は、ＩＣカードに格納されているデータを、ユーザの判断で退避させることを可能とすると共に、退避させてあるデータの不正使用を防止することを可能とすることにある。

【００１２】

【課題を解決するための手段】上記目的を達成するために、本発明は、ＩＣカードに格納されているデータを、ＩＣカード内で生成した暗号化鍵を用いてＩＣカード内で暗号化し、暗号化後のデータをＩＣカードから退避させるようにしている。また、生成した暗号化鍵をＩＣカード内で管理しておき、退避させておいたデータを回復させる際には、このデータを、ＩＣカード内で管理しておいた暗号化鍵を用いてＩＣカード内で復号するようにしている。

【００１３】すなわち、本発明は、第１の態様として、１つ以上のデータが内部のメモリに格納されているＩＣカードであって、退避対象とするデータの指定を外部から受け付ける手段と、任意の暗号化鍵を生成する手段と、退避対象として受け付けたデータを、生成した暗号化鍵を用いて暗号化すると共に、暗号化前のデータを消去する手段と、生成した暗号化鍵を記憶する手段と、暗号化後のデータを外部に退避させる手段と、退避させておいたデータを外部から受け取る手段と、受け取ったデータを、記憶しておいた暗号化鍵を用いて復号する手段と、復号後のデータを内部のメモリに再格納する手段とを備えたことを特徴としたＩＣカードを提供している。

【００１４】第１の態様によれば、ＩＣカードから退避させられたデータは、これを暗号化したＩＣカード以外では復号できないので、不正使用されることがなくなる。

【００１５】ここで、暗号化したデータをＩＣカードから退避させる必要がない場合には、暗号化前のデータを暗号化後のデータに置き換えるようにすればよい。

【００１６】すなわち、本発明は、第２の態様として、１つ以上のデータが内部のメモリに格納されているＩＣカードであって、無効化対象とするデータの指定を外部から受け付ける手段と、任意の暗号化鍵を生成する手段と、無効化対象として受け付けたデータを、生成した暗号化鍵を用いて暗号化すると共に、暗号化前のデータを暗号化後のデータに置き換える手段と、生成した暗号化鍵を記憶する手段と、有効化対象とするデータの指定を外部から受け付ける手段と、有効化対象として受け付けたデータを、記憶しておいた暗号化鍵を用いて復号する手段とを備えたことを特徴としたＩＣカードを提供している。

【００１７】なお、第１の態様および第２の態様のＩＣカードいずれにおいても、内部のメモリに格納されている１つ以上のデータは、ＡＰを含むようにすることができるのは、当然である。

【００１８】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照して説明する。

【００１９】図２は、本実施形態に係るＩＣカードシステムの全体構成図である。

【００２０】図２に示すように、本実施形態に係るＩＣカードシステムは、ユーザが所有するＩＣカード２０１と、端末装置２２１とが、ＩＣカードリーダ／ライタ２１１を介して接続された構成となっている。

【００２１】ＩＣカード２０１は、ＭＰＵ２０３と、メモリ２０２と、送受信ＩＦ２０４とを備えて構成され、端末装置２２１は、ＭＰＵ２２３と、メモリ２２２と、キーボード２２４と、ディスプレイ２２５と、送受信ＩＦ２２６とを備えて構成されている。

【００２２】また、ＩＣカードリーダ／ライタ２１１は、送受信ＩＦ２１２と、送受信ＩＦ２１３とを備えて構成されている。

【００２３】ＩＣカード２０１および端末装置２２１は、ＩＣカードリーダ／ライタ２１１を介して送受信を行うが、通信の形態は有線／無線を問わない。

【００２４】次に、ＩＣカード２０１のメモリ２０２に格納されている内容について、図３を用いて説明する。

【００２５】図３に示すように、ＩＣカード２０１のメモリ２０２には、例えば、クレジットやＧＳＭ（global system for mobile communication）等の、１つ以上ＡＰが格納されているが、ここでは、ＡＰ＃１（３２１）およびＡＰ＃２（３２２）が格納されているものとする。

【００２６】また、図３に示すように、ＩＣカード２０１のメモリ２０２には、ＩＣカード２０１ごとに固有の識別子であるカード識別子３１１と、非対称暗号における認証局の公開鍵３１２と、非対称暗号におけるＩＣカード２０１の秘密鍵３１３と、非対称暗号におけるＩＣカード２０１の公開鍵３１４と、ＡＰ管理情報３１５と、ＩＣカード２０１へのアクセスを許可するためのパスワード３１６とが格納されている。

【００２７】図７はＡＰ管理情報３１５の一例を示す図である。

【００２８】ＡＰ管理情報３１５は、ＩＣカード２０１のメモリ２０２に格納されているＡＰ（ここでは、ＡＰ＃１（３２１）およびＡＰ＃２（３２２）である。）の各々に対応するＡＰ管理データリスト７００から構成されている。

【００２９】図７に示すように、ＡＰ＃１（３２１）のＡＰ管理データリスト７００は、ＡＰ＃１（３２１）の識別子であるＡＰ識別子７０１と、ＡＰファイル情報７０２と、ＡＰ＃１（３２１）をＩＣカード２０１へロードした回数を示すロードカウンタ７０３と、ＡＰ＃１（３２１）をＩＣカード２０１からデリートした回数を示すデリートカウンタ７０４と、図８に示す退避データレコード８００へのポインタ７０５と、次のＡＰであるＡＰ＃２（３２２）のＡＰ管理データリスト７００へのエントリポインタ７０６とから構成されている。

【００３０】なお、ＡＰ＃２（３２２）のＡＰ管理データリスト７００も同様の構成である。

【００３１】また、ポインタ７０５には、対応するＡＰを退避させていないならば、「ＮＵＬＬ」が設定され、対応するＡＰを退避させているならば、退避データレコード８００へのポインタが、ＡＰの退避が完了した時点で設定される。なお、退避データレコード８００の詳細については後述する。

【００３２】図３に戻って、ＩＣカード２０１のメモリ２０２には、ＡＰ退避プログラム３０３と、ＡＰ回復プログラム３０４と、暗号化鍵生成プログラム３０５と、署名生成プログラム３０６と、対称暗号系暗号化／復号プログラム３０７と、非対称暗号系暗号化／復号プログラム３０８とが格納されている。

【００３３】次に、端末装置２２１のメモリ２２２に格納されている内容について、図４を用いて説明する。

【００３４】図４に示すように、端末装置２２１のメモリ２２２には、端末装置２２１ごとに固有の識別子である端末識別子４１１と、非対称暗号における認証局の公開鍵４１２とが格納されている。

【００３５】また、図４に示すように、端末装置２２１のメモリ２２２には、ＡＰ退避プログラム４０３と、ＡＰ回復プログラム４０４と、署名検証プログラム４０５と、対称暗号系暗号化／復号プログラム４０６と、非対称暗号系暗号化／復号プログラム４０７とが格納されている。

【００３６】なお、ＩＣカード２０１のメモリ２０２および端末装置２１１のメモリ２２２に格納される各種データは、各々、生成／発行／管理機関を設けることが考えられるが、ここでは、一般的に存在する認証局によって認証された公開鍵（認証局によって署名が施された公開鍵）を含む各種データが既に設定されているものとする。

【００３７】次に、本実施形態に係るＩＣカードシステムにおいて、ＩＣカード２０１に格納されているＡＰを端末装置２２１に退避させる際の動作について、図１を用いて説明する。

【００３８】図１は、本実施形態に係るＩＣカードシステムにおけるＡＰ退避時の動作の流れを示す図である。

【００３９】端末装置２２１でＡＰ退避プログラム４０３が起動され、ＩＣカード２０１がＩＣカードリーダ／ライタ２１１に挿入されると、ＩＣカード２０１でＡＰ退避プログラム３０３が起動され、以下の処理が実行される。なお、以下の処理は、ＩＣカード２０１のＭＰＵ２０３および端末装置２２１のＭＰＵ２２３が、ＡＰ退避プログラム３０３およびＡＰ退避プログラム４０３を実行することで実現される。

【００４０】まず、ＩＣカード２０１および端末装置２１１は、相互認証を行う（ステップ１００，ステップ１１０）。相互認証については、例えば、ＩＳＯ（ＩＳＯ９７９８－３）に、非対称鍵暗号を用いた認証方式が規定されており、また、ＩＳＯ（ＩＳＯ９７９８－２）に、対称鍵暗号を用いた認証方式が規定されているので、ここでは詳細を省略する。

【００４１】続いて、ＩＣカード２０１および端末装置２１１は、本人認証を行う（ステップ１０１，ステップ１１１）。

【００４２】本人認証においては、詳しくは、まず、端末装置２２１が、ディスプレイ２２５を介して、パスワードの入力をユーザに要求し、ユーザがキーボード２２４から入力したパスワードを、ＩＣカード２０１に送信する（ステップ１１１）。

【００４３】そして、ＩＣカード２０１が、端末装置２１１からパスワードを受信すると、受信したパスワードとメモリ２０２に格納されているパスワード３１６とを比較し、正しいユーザであるか否かを認証する（ステップ１０１）。なお、ＩＣカード２０１による認証結果は、端末装置２１１に通知される。

【００４４】さて、正しいユーザであることが認証された場合は、ＩＣカード２０１および端末装置２１１は、退避対象ＡＰの指定を行う（ステップ１０２，ステップ１１２）。

【００４５】退避対象ＡＰの指定においては、詳しくは、まず、端末装置２２１が、ＩＣカード２０１に格納されているＡＰの一覧を、ＩＣカード２０１から取得し

てディスプレイ２２５に表示し、ユーザがキーボード２２４から指定したＡＰを、退避対象ＡＰとして、ＩＣカード２０１に通知する（ステップ１１２）。なお、退避対象ＡＰの通知は、図５に示すＡＰ指定データレコード５００を送信することで行われる。

【００４６】図５はＡＰ指定データレコード５００の一例を示す図である。

【００４７】図５に示すように、ＡＰ指定データレコード５００は、退避対象ＡＰを一意に指定するための識別子であるＡＰ識別子５０１と、端末装置２２１の端末識別子（メモリ２２２に格納されている端末識別子４１１）５０２と、退避対象ＡＰの指定を端末装置２２１が受け付けた日時を示すタイムスタンプ５０３とから構成されている。

【００４８】そして、ＩＣカード２０１が、端末装置２１１からＡＰ指定データレコード５００を受信することで、退避対象ＡＰの指定を受け付ける（ステップ１０２）。

【００４９】続いて、ＩＣカード２０１は、ＡＰ指定データレコード５００を受信すると、暗号化鍵生成プログラム３０５を起動することによって、退避対象ＡＰを暗号化するための暗号化鍵を生成する（ステップ１０３）。ここでは、退避対象ＡＰを対称暗号で暗号化するものとし、生成する暗号化鍵は、対称暗号における暗号化鍵（例えば、乱数）である。

【００５０】続いて、ＩＣカード２０１は、対称暗号系暗号化／復号プログラム３０８を起動することによって、ステップ１０３で生成した暗号化鍵を用いて、退避対象ＡＰを暗号化すると共に、暗号化前のＡＰを消去する（ステップ１０４）。

【００５１】続いて、ＩＣカード２０１は、署名生成プログラム３０６を起動することによって、署名を生成する（ステップ１０５）。

【００５２】ステップ１０５では、詳しくは、ＩＣカード２０１は、図９に示す署名生成用データレコード９００から、ハッシュ関数を用いて認証子を生成し、非対称暗号系暗号化／復号プログラム３０８を起動することによって、メモリ２０２に格納されているＩＣカード２００の秘密鍵３１３を用いて、生成した認証子を暗号化して、署名を生成する。なお、ハッシュ関数および署名生成の詳細は、例えば、岡本龍明他著「現代暗号」，産経図書発行を参照されたい。

【００５３】図９は署名生成用データレコード９００の一例を示す図である。

【００５４】図９に示すように、署名生成用データレコード９００は、退避対象ＡＰのＡＰ識別子９０１と、暗号化した退避対象ＡＰ９０２と、端末識別子（端末装置２２１から受信したＡＰ指定データレコード５００中の端末識別子５０２）９０３と、タイムスタンプ（端末装置２２１から受信したＡＰ指定データレコード５００中のタイムスタンプ５０３）９０４と、ＩＣカード２０１のカード識別子（メモリ２０２に格納されているカード識別子３１３）９０５とから構成されている。

【００５５】続いて、ＩＣカード２０１および端末装置２１１は、暗号化した退避対象ＡＰの送受信を行う（ステップ１０６，ステップ１１３）。

【００５６】暗号化した退避対象ＡＰの送受信においては、詳しくは、まず、ＩＣカード２０１が、暗号化した退避対象ＡＰを、端末装置２２１に送信する（ステップ１０６）。なお、暗号化した退避対象ＡＰの送信は、図６に示す退避ＡＰデータレコード６００を送信することで行われる。

【００５７】図６は退避ＡＰデータレコード６００の一例を示す図である。

【００５８】図６に示すように、退避ＡＰデータレコード６００は、暗号化した退避対象ＡＰのＡＰ識別子６０１と、ステップ１０４で暗号化した退避対象ＡＰ６０２と、ＩＣカード２０１のカード識別子（メモリ２０２に格納されているカード識別子３１３）６０３と、ステップ１０５で生成した署名６０４と、ＩＣカード２０１の公開鍵６０５（メモリ２０２に格納されている公開鍵３１４）とから構成されている。

【００５９】そして、端末装置２２１が、ＩＣカード２０１から退避ＡＰデータレコード６００を受信することで、暗号化された退避対象ＡＰを受信する（ステップ１１３）。

【００６０】さて、端末装置２２１は、退避ＡＰデータレコード６００を受信すると、署名検証プログラム４０５を起動することによって、退避ＡＰデータレコード６００中の署名６０４を検証する（ステップ１１４）。

【００６１】ステップ１１４では、詳しくは、端末装置２２１は、非対称暗号系暗号化／復号プログラム４０７を起動することによって、まず、退避ＡＰデータレコード６００中の公開鍵６０５を、認証局の公開鍵４１２を用いて復号して、公開鍵６０５を検証し、続いて、退避ＡＰデータレコード６００中の署名６０４を、検証した公開鍵６０５を用いて復号して、署名６０４を検証する。

【００６２】そして、端末装置２２１は、ステップ１１４による検証の結果、退避ＡＰデータレコード６００がＩＣカード２０１から送信されたものであること、および、退避ＡＰデータレコード６００が改ざんされていないことを確認すると、退避ＡＰデータレコード６００を、メモリ２２２またはディスク装置等に格納する（ステップ１１５）。なお、端末装置２２１は、ＡＰの退避に成功した旨をＩＣカード２０１に通知する。

【００６３】そこで、ＩＣカード２０１は、ＡＰの退避に成功した旨が端末装置２２１から通知されると、対応するＡＰ管理データリスト７００を更新する（ステップ１０７）。

【００６４】ステップ１０７では、具体的には、ＩＣカード２０１は、退避データレコード８００を生成し、生成した退避データレコード８００へのポインタを、対応するＡＰ管理データリスト７００中のポインタ７０５に設定する。

【００６５】図８は退避データレコード８００の一例を示す図である。

【００６６】図８に示すように、退避データレコード８００は、端末識別子（端末装置２２１から受信したＡＰ指定データレコード５００中の端末識別子５０２）８０１と、タイムスタンプ（端末装置２２１から受信したＡＰ指定データレコード５００中のタイムスタンプ５０３）８０２と、ステップ１０３で生成した暗号化鍵８０３と、ステップ１０５で生成した署名８０４とから構成されている。

【００６７】以上に説明した動作によって、ＩＣカード２０１に格納されているＡＰを、端末装置２２１に退避させることができる。

【００６８】なお、図１に示した動作においては、対称暗号で退避対象ＡＰを暗号化するようにしているが、非対称暗号で退避対象ＡＰを暗号化するようにしてもよい。この場合には、ＩＣカード２０１は、ステップ１０３では、非対称暗号のアルゴリズムに応じた暗号化鍵を生成するようにする。

【００６９】また、図１に示した動作において、ＩＣカード２０１および端末装置２２１は、ステップ１００およびステップ１１０の相互認証の過程で、一時鍵を共有することができるので、退避ＡＰデータレコード６００を、この一時鍵を用いて暗号通信するようにしてもよい。

【００７０】また、図１に示した動作において、端末装置２２１は、ユーザに退避場所を指定させるようにし、ユーザがキーボード２２４から指定した場所に、退避ＡＰデータレコード６００を格納するようにしてもよい。

【００７１】また、図１に示した動作においては、セキュリティ性をより高めるために、署名による認証技術を利用して、退避ＡＰデータレコード６００がＩＣカード２０１から送信されたものであること、および、退避ＡＰデータレコード６００が改ざんされていないことを確認するようにしているが、これによって本発明の主旨が限定されることはない。

【００７２】次に、本実施形態に係るＩＣカードシステムにおいて、図１に示した動作で退避させたＡＰを回復させる際の動作について、図１０を用いて説明する。

【００７３】図１０は、本実施形態に係るＩＣカードシステムにおけるＡＰ回復時の動作の流れを示す図である。

【００７４】端末装置２２１でＡＰ回復プログラム４０４が起動され、ＩＣカード２０１がＩＣカードリーダ／ライタ２１１に挿入されると、ＩＣカード２０１でＡＰ回復プログラム３０４が起動され、以下の処理が実行される。なお、以下の処理は、ＩＣカード２０１のＭＰＵ２０３および端末装置２２１のＭＰＵ２２３が、ＡＰ回復プログラム３０４およびＡＰ回復プログラムを実行することで実現される。

【００７５】まず、ＩＣカード２０１および端末装置２１１は、図１で説明した動作と同様に、相互認証を行い（ステップ１００，ステップ１１０）、本人認証を行う（ステップ１０１，ステップ１１１）。

【００７６】そして、正しいユーザであることが認証された場合は、ＩＣカード２０１および端末装置２１１は、回復対象ＡＰの指定を行う（ステップ１００２，ステップ１０１２）。

【００７７】回復対象ＡＰの指定においては、詳しくは、まず、端末装置２２１が、ＩＣカード２０１に格納されているＡＰのうちの、退避中のＡＰの一覧を、ＩＣカード２０１から取得してディスプレイ２２５に表示し、ユーザがキーボード２２４から指定したＡＰを、回復対象ＡＰとして、ＩＣカード２０１に通知する（ステップ１０１２）。なお、回復対象ＡＰの通知は、退避対象ＡＰの通知と同様に、ＡＰ指定データレコード５００を送信することで行われる。

【００７８】そして、ＩＣカード２０１が、端末装置２１１からＡＰ指定データレコード５００を受信することで、回復対象ＡＰの指定を受け付ける（ステップ１００２）。

【００７９】続いて、ＩＣカード２０１は、ＡＰ指定データレコード５００を受信すると、回復対象ＡＰのＡＰ管理データリスト７００、および、該ＡＰ管理データリスト７００中のポインタ７０５が示す退避データレコード８００を取り出す（ステップ１００３）。

【００８０】続いて、ＩＣカード２０１および端末装置２１１は、回復対象ＡＰの送受信を行う（ステップ１００４，ステップ１０１３）。

【００８１】回復対象ＡＰの送受信においては、詳しくは、まず、端末装置２１１が、メモリ２２２またはディスク装置等に格納しておいた退避ＡＰデータレコード６００を、回復対象ＡＰとして、端末装置２２１に送信する（ステップ１０１３）。そして、ＩＣカード２０１が、端末装置２１１から退避ＡＰデータを受信することで、回復対象ＡＰを受信する（ステップ１００４）。

【００８２】さて、ＩＣカード２０１は、退避ＡＰデータレコード６００を受信すると、退避ＡＰデータレコード６００中の署名６０４と、ステップ１００３で取り出した退避データレコード８００中の署名８０４とが一致するか否かを確認する（ステップ１００５）。

【００８３】そして、ＩＣカード２０１は、両者が一致することを確認すると、対称暗号系暗号化／復号プログラム３０７を起動することによって、受信した退避ＡＰデータレコード６００中の暗号化ＡＰ６０２を、ステッ

プ１００３で取り出した退避データレコード８００中の暗号化鍵８０３を用いて復号し、復号した回復対象ＡＰを、ステップ１００３で取り出したＡＰ管理データリスト７００中のファイル情報７０２に従って、メモリ２０２内に再配置する（ステップ１００６）。

【００８４】さらに、ＩＣカード２０１は、回復対象ＡＰのＡＰ管理データリスト７００を更新する（ステップ１００７）。

【００８５】ステップ１００７では、具体的には、ＩＣカード２０１は、ステップ１００３で取り出した退避データレコード８００を消去し、回復対象ＡＰのＡＰ管理データリスト７００中のポインタ７０５に「ＮＵＬＬ」を設定する。

【００８６】以上に説明した動作によって、端末装置２２１に退避させておいたＡＰを、ＩＣカード２０１に回復させることができる。

【００８７】以上説明したように、本実施形態に係るＩＣカードシステムによれば、ＩＣカード２０１に格納されているＡＰを、ユーザの判断で、ＩＣカード２０１から端末装置２２１に退避させることが可能になる。そして、退避対象ＡＰを、ＩＣカード２０１内で生成した暗号化鍵を用いて暗号化するようにしているので、ＩＣカード２０１から退避させられたＡＰは、これを暗号化したＩＣカード２０１以外では復号できず、不正使用されることがない。

【００８８】そこで、特に、ＩＣカード２０１が、ＭＵＬＴＯＳをカードＯＳとしている場合でも、図１に示した動作を行うことで、ユーザの判断で、一時的にＡＰを退避させるようなフレキシブルな運用を実現することができる。

【００８９】ところで、本実施形態に係るＩＣカードシステムにおいては、ＩＣカード２０１に格納されているＡＰを、端末装置２２１に退避させるようにしているが、ＩＣカード２０１のメモリ２０２に余裕がある場合など、暗号化したＡＰをＩＣカード２０１から退避させる必要がない場合には、ＡＰを退避させる代わりに、ＩＣカード２０１内でＡＰを一時的に無効化するようにすることができる。

【００９０】以下、このようにした場合の動作について、図１１を用いて説明する。

【００９１】図１１は、本実施形態に係るＩＣカードシステムにおけるＡＰ無効化時の動作の流れを示す図である。

【００９２】図１１に示す動作は、図１に示した動作と同様であるが、ステップ１１０６において、ＩＣカード２０１が、暗号化したＡＰを、ＩＣカード２０１内に格納するようにした点が異なる。そこで、上述した各種データにおいて、退避／回復させるために必要であった部分には、何も設定されないこととなる。

【００９３】図１１に示した動作によれば、ＡＰを実際には退避させていないが、ＩＣカード２０１内でＡＰを暗号化しているので、第三者の脅威から護ることができる。

【００９４】なお、無効化されたＡＰを有効化する際の動作は、ＩＣカード２０１が、暗号化されて無効化されているＡＰを、これを暗号化したときに用いた暗号化鍵を用いて復号すればよい。

【００９５】また、図１１に示した動作を行うようにする場合には、端末装置２２１において、ＡＰを退避させるか、または、無効化させるかという選択を、ユーザに指定させるようにする必要がある。

【００９６】また、図１１に示した動作は、図１に示した動作とは独立に行うことが可能である。すなわち、図１１に示した動作のみを行うＩＣカードシステムを構築することが可能である。

【００９７】なお、以上の説明では、退避対象および無効化対象とするデータがＡＰであるものとしているが、ＡＰ以外の他のデータであってもよいことは、説明するまでもない。

【００９８】

【発明の効果】以上説明したように、本発明によれば、ＩＣカードに格納されているデータを、ユーザの判断で、ＩＣカードから退避させることが可能になる。そして、退避させるＡＰを、ＩＣカード内で生成した暗号化鍵を用いて暗号化するようにしているので、ＩＣカードから退避させられたデータは、これを暗号化したＩＣカード以外では復号できず、不正使用されることがない。

【図面の簡単な説明】

【図１】本実施形態に係るＩＣカードシステムにおけるＡＰ退避時の動作の流れを示す説明図。

【図２】本発明の実施形態に係るＩＣカードシステムの全体構成図。

【図３】本発明の実施形態におけるＩＣカードのメモリに格納されている内容を示す説明図。

【図４】本発明の実施形態における端末装置のメモリに格納されている内容を示す説明図。

【図５】本発明の実施形態におけるＡＰ指定データの一例を示す説明図。

【図６】本発明の実施形態における退避ＡＰデータの一例を示す説明図。

【図７】本発明の実施形態におけるＡＰ管理情報の一例を示す説明図。

【図８】本発明の実施形態における退避データの一例を示す説明図。

【図９】本発明の実施形態における署名生成用データの一例を示す説明図。

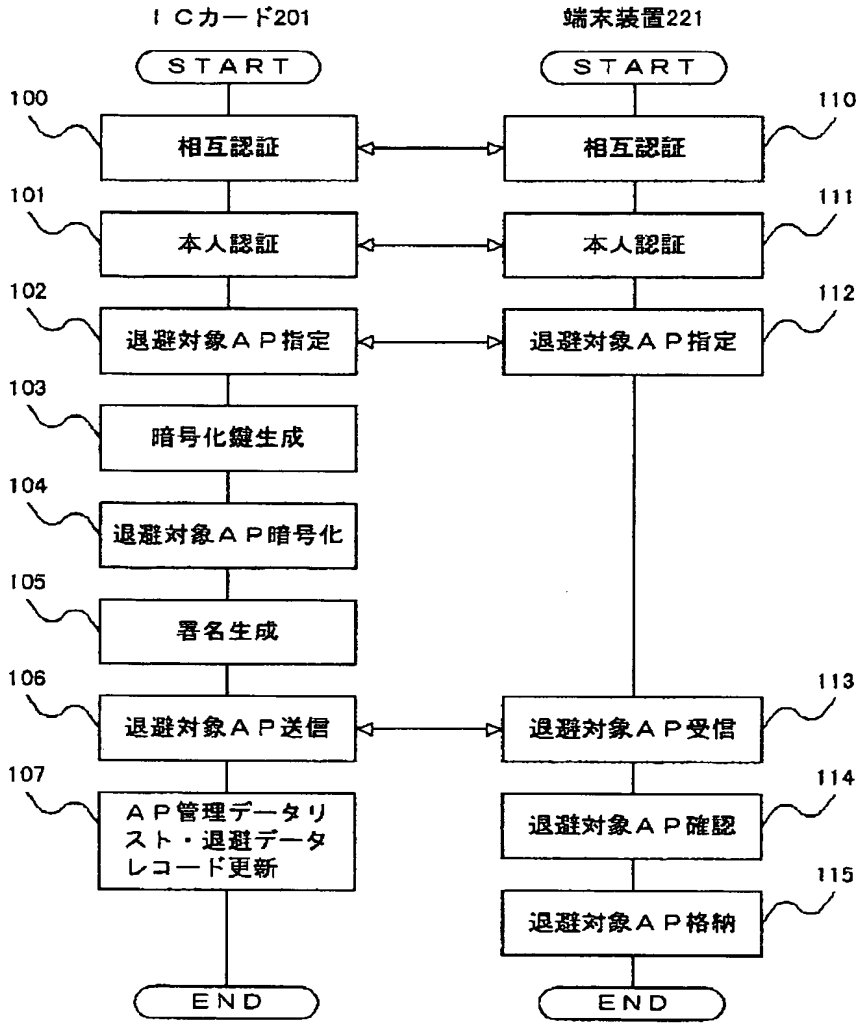
【図１０】本実施形態に係るＩＣカードシステムにおけるＡＰ回復時の動作の流れを示す説明図。

【図１１】本実施形態に係るＩＣカードシステムにおけるＡＰ無効化時の動作の流れを示す説明図。

【符号の説明】
２０１…ＩＣカード、２１１…ＩＣカードリーダ／ライタ、２２１…端末装置、２０２，２２２…メモリ、２０３，２２３…ＭＰＵ、２０４，２１２，２１３…送受信ＩＦ、２２４…キーボード、２２５…ディスプレイ、５００…ＡＰ指定データレコード、６００…退避ＡＰデータレコード、７００…ＡＰ管理データリスト、８００…退避データレコード、９００…署名生成用データレコード。

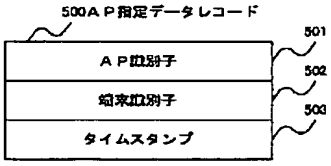
【図１】

図 1



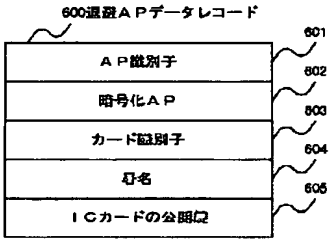
【図５】

図 5



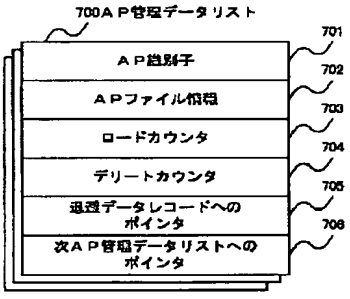
【図６】

図 6



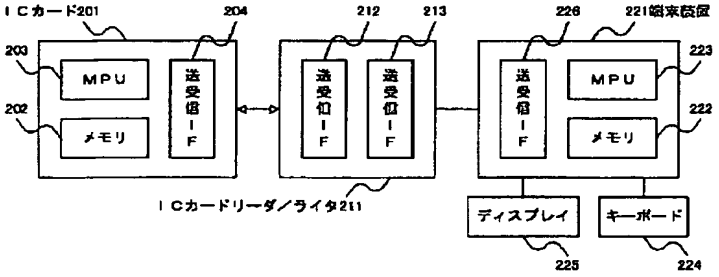
【図７】

図 7



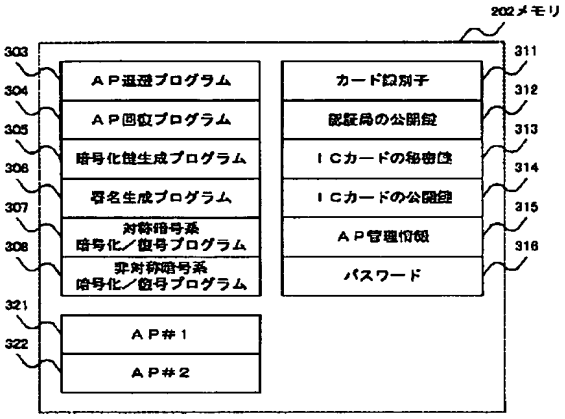
【図2】

図 2



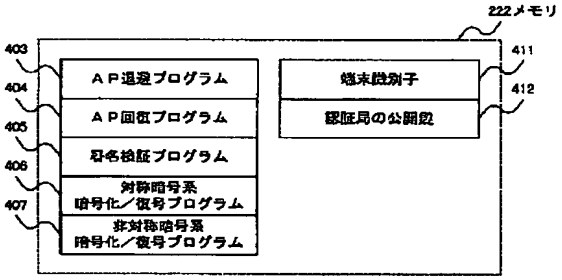
【図3】

図 3



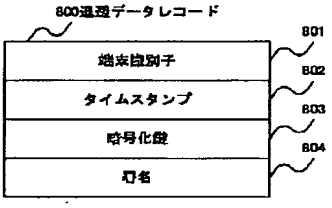
【図4】

図 4



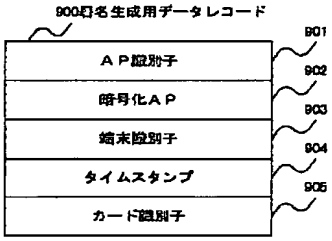
【図8】

図 8



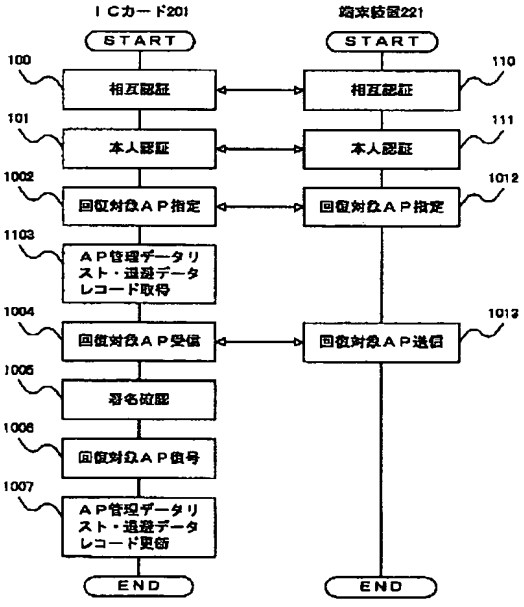
【図9】

図 9



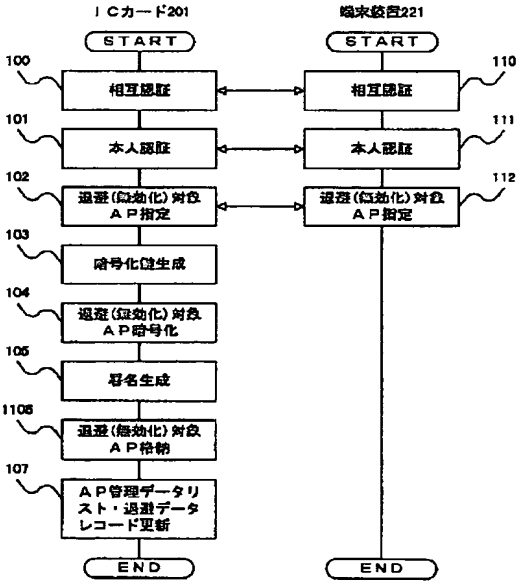
【図10】

図 10



【図11】

図 11



フロントページの続き

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｋ　19/07		Ｇ０６Ｋ　19/00	Ｎ	

(72)発明者　原口　政敏
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

Ｆターム(参考)　5B035 AA13 BB09 BC03 CA29 CA38
5B058 CA27 KA01 KA04 KA35 YA13
5B065 BA09 PA16